Outline: Privacy Rule

45 CFR Subtitle A, Subchapter C

Revisions to part 160 as follows:

Subpart A: General Provisions

160.101 Statutory basis and purpose.

Implements sections 1171 through 1179 of the Social Security Act (the Act)

160.102 Applicability

Except as otherwise provided (160.300), rule applies to "Covered Entities", definition consistent with the Transactions rule.

160.103 Definitions

Term	Definition	Exception(s)
Act	Social Security Act	
ANSI	American National Standards Institute	
Business Associate (B.A.)	**If B.A** (not a member of entity's workforce) who performs/assists in these activities on behalf of entity: • Claims processing or administration • Data analysis • Utilization Review • Quality assurance • Billing • Benefit management • Practice management • Repricing • Legal • Actuarial • Accounting, Financial Svcs. • Consulting • Data Aggregation • Management/Administrative • Accreditation **Receives PHI (Protected Health Information) from the entity,** or the entity's other B.A in the performance of these services, **then the B.A. must follow the rule.** A covered entity can be a B.A. for another covered entity.	
Compliance Date	Date covered entities must comply	
Covered Entity	Health Plan Health care clearinghouse Provider who transmits any health information in electronic form in connection with a (HIPAA) transaction	

Group Health Plan	As defined in section 3(1) of ERISA to the extent that the plan provides medical care as defined in sec.2791(a)(2) of the PHS Act • Has 50 or more participants • Administered by an entity other than the employer	
HCFA	Health Care Financing Administration	
HHS	Department of Health and Human Services	
Health Care	Care, services, supplies related to the health of the individual	
Health Care Clearinghouse	Public or private entity: • Billing service • Repricing company • Community health MIS • VANs and switches That facilitate processing of non-standard data into standard data (data content or format)	
Health Care Provider	• Provider of services(sec.1861u of the Act) • Provider of medical or health services(sec.1861s of the Act) • Any other person/org. who furnishes, bills, or gets paid for health care	
Health Information	**Any information, <u>whether oral or recorded in any form</u> or medium, that is created or received by:** • Health care provider • Health plan • Public health authority • Employer • Life insurer • School/university • Health care clearinghouse **And relates to:** • Past, present, or future physical/mental health/condition of individual • Provision of health care to an individual • Past, present, or future payment for an individual's health care	
Health insurance issuer	• Insurance company • Insurance service • Insurance organization (HMO) Licensed by a State and who is subject to State law regulating insurance. This term does not include a group health plan.	
Health Maintenance Organization	Federally qualified HMO	

(HMO)	State-recognized HMO, or similar organization regulated under State law	

Health Plan (revised definition; omits the following sentence from previous rule: "Health plan includes, when applied to government programs, the components of the government agency administering the program.")	• Group health plan
	• Health insurance issuer
	• HMO
	• Medicare A, B, and C, plus Medigap
	• Medicaid
	• Issuer of long-term care policy
	• Employee welfare benefit plan
	• Veterans, CHAMPUS
	• Indian Health
	• FHP (federal employee)
	• State child health plan under title XXI of the Act
	• High risk pool established under State law
		• Any policy, plan or program that provides excepted benefits listed in sec. 2791(c 1) of the PHS Act
		  • Whose purpose is other than providing or paying for health care
		  OR
		  • Whose principal activity is
		  • Direct provision of healthcare to persons
		  • Making of grants to fund direct provision of healthcare to persons

Implementation specification	Specific requirements or instructions for implementing a standard.	
Modify or modification	Change adopted by the Secretary, through regulation, to a standard or implementation specification	
Secretary	• Secretary of HHS • Any officer or employee of HHS (with delegated authority)	
Small health plan	Health plan with annual receipts of $5 million or less	
Standard	A rule, condition, or requirement, for products, systems, services or practices: • Classification of components • Materials, performance, operations specs • Delineation of procedures **OR** **With respect to the privacy of individually identifiable information.**	
Standard setting organization (SSO)	ANSI-accredited organization that maintains standards for • Information transactions • Data elements • Any other standard necessary to implement this part	
State	• For a health plan established/regulated by Federal law, see applicable section of United States Code	

	• For all other purposes: the 50 states + Puerto Rico, Virgin Islands, and Guam.	
Trading partner agreement	Agreement related to the electronic exchange of information	
Transaction	Transmission of information between two parties to carry out financial/administrative activities related to health care. Includes • Transactions named in HIPAA transactions rule • Health claims attachments • Other transactions prescribed by future regs	
Workforce	Employees, volunteers, trainees, and others whose work performance is under the direct control of the covered entity, whether or not they are paid by the covered entity.	

160.104 Modifications
Secretary may adopt modification to a standard or implementation specification

- No more than once every 12 months
- Any time after during the first year the standard or spec is adopted
- Secretary establishes the compliance date for the modified standard
    - No earlier than 180 days after effective date of final rule
    - Secretary may extend compliance date

Subpart B: Preemption of State Law

160.201 Applicability
Provisions of this subpart implement section 1178 of the Act

160.202 Definitions

Contrary	When used to compare State law to a standard/requirement/spec (adopted under HIPAA) , ***contrary*** means: • The covered entity would find it impossible to comply with both State and Federal requirements, **OR** • The State law stands as an obstacle to compliance with part C, title XI of the Act or section 264 of PL 104-191, as applicable

More stringent
(Note: California law AB416 is more stringent; applies to all individuals, not only "covered entities", and does allow individuals a private right of action)
	When comparing State law to a standard (ref. Subpart E of part 164 of this subchapter), **when the State law meets one or more of the following criteria:**
	• The State law prohibits a disclosure permitted under the (Federal) rule
	• The State law allows the individual greater rights of access or amendment to one's personal PHI
	• The State law provides the individual with a greater amount of information than the Federal law, regarding use/disclosure/rights and remedies
	• The State law regarding the form/content of the authorization/consent form for use and disclosure of PHI provides more privacy protection, narrows the scope or duration of the consent, or reduces the coercive effect of circumstances surrounding the auth/consent
	• For record-keeping or accounting of disclosures, the State law requires a longer records retention period , or requires more detailed information be provided to the individual.
	• The State law provides greater privacy protection for the individual who is the subject of the PHI.
	If one or more of these criteria are met, the State law is not pre-empted.
	
	Note: If the State law prohibits or authorizes disclosure of protected health information about a minor to a parent or guardian, the Federal law does not pre-empt the State law.
	
	• **EXCEPTIONS to "More Stringent":**
	  • When disclosure is required by the Secretary in reviewing a covered entity's (privacy) compliance
	  • When disclosing to the individual who is the subject of the PHI (protected health information.

Relates to the privacy of individually identifiable health information (with respect to State law)	The State law has the specific purpose of protecting the privacy of health information
State law	Constitution, statute, regulation, rule, common law, or other State action that has the force and effect of law.

160.203 General rule and exceptions

General Rule: Where a standard / requirement / spec adopted under this subchapter is **contrary** to a provision of State law, the Federal rule pre-empts the State law.

Exceptions to preemption of State law: Where the Secretary determines that the provision of State law

- Is necessary to prevent fraud/abuse, or to ensure appropriate State regulation of insurance/health plans
- For State reporting on health care delivery or costs
- When a standard/requirement/spec (under part 164)is at issue, and the Secretary determines that intrusion into privacy is warranted when balanced against a compelling public need (public health, safety or welfare)
- When the principal purpose of the State law regulates "controlled substances" as defined by State law
- When the State law relates to privacy of health information and is more stringent
- When the State law provides for reporting of disease, injury, child abuse, birth, or death; for public health surveillance, investigation, intervention
- When State law requires a health plan to provide access to information for audits, monitoring/evaluation, licensure or certification of facilities or individuals

160.204 Process for requesting exception determinations

- Submit a written request to except a provision of State law from Federal preemption. Statement must include the following information:
  - The State law pertinent to the request
  - Which standard/requirement/spec (of the privacy rule) the request pertains to
  - Which part of the standard is not being implemented
  - How health care providers, health plans, and other entities will be affected by the exception
  - Reasons why the State law should not be preempted, and which exception criteria from section 160.203 were met
  - Any other information the Secretary may request in order to make the determination.
- Address for submitting exception requests will be published in the Federal Register. Until the determination is made by the Secretary, the (Federal) standard remains in effect.
- Secretary's determination will be based on the information provided in the request, and how well the request meets the criteria of section 160.203.

160.205 Duration of effectiveness of exception determinations

An exception granted remains in effect until:

- The State law or the Federal standard is materially changed so that the basis for exception no longer exists
- The Secretary determines that the basis for exception no longer exists

Subpart C: Compliance and Enforcement

160.300 Applicability

The "Compliance and Enforcement" section applies to actions by:

- The Secretary
- Covered Entities
- Others

In ascertaining the compliance by covered entities.

Applies to the enforcement of requirements under this part 160 (General Requirements) and subpart E of part 164 (privacy of individually identifiable health information).

160.301 Definitions (for subpart C)

Same meaning as defined in section 164.501 (Privacy of IIHI)

160.304 Principles for achieving compliance

Cooperation — Secretary will seek the cooperation of covered entities
Assistance — Secretary may provide technical assistance to covered entities to help them comply

160.305 Complaints to the Secretary

Right to file a complaint

A person who believes a covered entity is not in compliance may file a complaint with the Secretary

Requirements for filing a complaint

- Complaint must be written (paper or electronic document)
- Complaint must name the entity, describe the acts or omissions leading to the complaint
- Complaint must be filed within 180 days of the occurrence. Secretary has discretion to waive the time limit.
- Secretary may prescribe additional procedures for filing a complaint, by publishing notice in the Federal Register.
- Secretary may investigate complaints.

160.308 Compliance reviews

The Secretary may conduct compliance reviews to determine compliance by covered entities.

160.310 Responsibilities of covered entities

Provide records and compliance reports

- Covered entity must keep these records
- Covered entity must furnish these records at the Secretary's request

Cooperate with complaint investigations and compliance reviews

- Covered entity must cooperate with the Secretary in investigation or compliance review

Permit access to information

- Covered entity must permit access by Secretary during normal business hours, and permit access to **all** facilities and sources of information, including protected health information, that are pertinent to ascertaining compliance. If the Secretary believes "exigent circumstances" exist (documents might be hidden or destroyed), entity must permit Secretary access at any time and without notice.
    - If the pertinent information is in the possession of some other person/entity, and they fail or refuse to furnish the information, the covered entity must certify what efforts it has made to obtain the information.
    - Protected information obtained during an investigation or compliance review will not be disclosed by the Secretary, except as necessary for ascertaining or enforcing compliance, or if otherwise required by law.

160.312 Secretarial action regarding complaints and compliance reviews

Resolution where noncompliance is indicated

- Secretary will inform the covered entity in writing and attempt to resolve the matter by informal means
- If the matter cannot be resolved informally, Secretary may issue written findings documenting the noncompliance to the covered entity (and to the complainant, if applicable)

No violation found

- If the Secretary determines that further action is not warranted, Secretary will inform the covered entity in writing (and complainant, if applicable).

Part 164 – Security and Privacy

Subpart A – General Provisions

164.102 Statutory Basis

The provisions of this part are adopted pursuant to the Secretary's authority under part C of title XI of the Act and section 264 of PL 104-191.

164.103 Applicability

Except as otherwise provided**,** applies to covered entities who transmit health information in electronic form

164.106 Relationship to the other parts

Covered entities must also comply with parts 160 and 162 of this subchapter.

Subpart B – D {Reserved}

Subpart E – Privacy of Individually Identifiable Health Information

164.500 Applicability

Except as otherwise provided, this subpart applies to covered entities

Health care clearinghouses must comply as follows:

- When a clearinghouse receives or creates protected health information as a business associate of a covered entity, clearinghouse must comply with:
    - Applicability, Section 164.500
    - Definitions, Section 164.501
    - Section 164.502 relating to use and disclosure, EXCEPT: Clearinghouse may only use or disclose information as permitted in the business associate contract
    - Transition requirements, section 164.532
    - Compliance dates for implementation, section 164.534
- When a clearinghouse receives/creates protected health info outside of the "business associate of a covered entity" role, then the clearinghouse must comply with **all** requirements of this subpart.

Exception:

- Does not apply to Department of Defense (or any agency acting on its behalf) when providing health care to overseas foreign national beneficiaries.

164.501 Definitions

Correctional institution	Any penal or correctional facility, jail, reformatory, detention center, halfway house or residential community program for confinement/rehabilitation of persons charged with or convicted of a criminal offense, or other persons held in lawful custody (includes delinquent juveniles, aliens awaiting deportation, persons committed to mental institutions via criminal justice system, witnesses, or others awaiting charges or trial.
Covered functions	Functions that make you a covered entity.
Data Aggregation	Protected health information received by business associate from several entities and combined for the purpose of data analyses related to healthcare operations.
Designated record set	A group of records maintained by/for the covered entity: • Medical records, billing records • Enrollment, payment, claims adjudication, case/medical management record systems used to make decisions about

	individuals
Direct treatment relationship	Between a provider and individual, "not an indirect treatment relationship".
Disclosure	Release, transfer, giving access to, divulging in any manner outside the entity holding the information
Health Care Operations	Definition consistent with Transactions rule
Health Oversight Agency	Definition consistent with Transactions rule
Indirect treatment relationship	Examples: 1)Provider A orders Provider B to deliver health services to the patient; 2) Diagnostic tests ordered by Provider A, tests conducted by Provider B, provider B gives result to the patient. *In both examples, Provider B has the indirect treatment relationship with the patient.*
Individual	The subject of protected health information
Individually Identifiable Health Information	A subset of health information that: • Is created by a covered entity or employer • Relates to present, past, or future health of individual • Relates to past, present, or future payment for healthcare • Identifies the individual
Inmate	Person confined to a correctional institution
Law enforcement official	Officer/employee (Federal, State, territory, tribal gov't) empowered to investigate or prosecute violation of law
Marketing	Communication about a product/service to encourage purchase. Excludes: • Benefit plan coverage descriptions • Treatment recommendations/options given by the provider
Organized Health care arrangement	Clinically integrated care setting where patients receive care from more than one provider; which has shared administrative and financial functions.
Payment	Includes billing, adjudication, eligibility determination, underwriting, premium payment , collections, utilization review
Protected Health Information	PHI that is **transmitted electronically, or maintained in any form.** Excludes: Education records
Psychotherapy notes	Mental health professional's notes, recorded in any medium, which document counseling/ treatment sessions and are kept separate from the medical record.
Public health authority	Agency or authority of U.S., State, territory, tribe, or person under authority, that is responsible for public health matters
Required by law	Mandate that compels a covered entity to disclose protected information, and that is enforceable by law.
Research	A systematic investigation designed to contribute to generalizable knowledge. Includes research development, testing, and evaluation.
Treatment	Provision, coordination, management of health care services
Use	Sharing/application, analysis within an entity that maintains PHI

164.502 Uses and disclosures of protected health information: General rules

Covered entities may not use/disclose PHI (Protected health information), except as permitted by this section and subpart C of part 160.

Permitted disclosures:

- To the individual

- With a consent, to carry out treatment / payment / healthcare operations
- Without consent, to carry out treatment / payment / healthcare operations, by a provider with an indirect treatment relationship to the patient, or in the course of providing care to an inmate, except psychotherapy notes
- With a specific, valid authorization (164.508)
- With the individual's informed agreement (164.510)
- In compliance with 164.512 or 164.514 (e),(f),(g)
  (Disclosures; required by law, public health activities, worker's comp, health oversight)

Required disclosures:
- To the individual
- To the Secretary as part of an investigation

Minimum necessary

Applies to:
- Disclosures between covered entities; make reasonable efforts to give only the minimum necessary information to accomplish the intended purpose of the request

Does not apply to disclosures made:
- to a provider for treatment
- to the individual
- to the Secretary
- as required by law enforcement

Disclosures subject to agreed upon restriction

If a covered entity has agreed (with the individual) to restrict certain information it must do so, except as provided in 164.522(a) (an emergency situation).

Disclosure / use of de-identified information
- OK to disclose to a business associate (standard for "de-identified" at 164.514)
- Cannot provide a "key" to re-identify the information.
- If the covered entity re-identifies the information, then PHI disclosure rules apply.

Disclosures to business associates

A covered entity may disclose to business associate to create or receive PHI on its behalf, **IF** the covered entity has reasonable assurance the business associate will not misuse the information.
Must have a written contract / agreement with the business associate that complies with the standard for B.A. agreements in 164.504.

Does not apply to:
- Health plan to provider disclosure concerning treatment of an individual
- Disclosure by health plan/issuer/HMO to plan sponsor
- **Disclosure by government health plan to an agency that determines enrollment/eligibility for the health plan (agency that is not the administrator of the health plan)**
- A covered entity that is in violation of the business partner agreement

Deceased individuals.

For the covered entity, disclosure rules apply to deceased and living individuals.

Personal representatives

A covered entity must recognize the individual's personal representative as the individual. Personal rep. defined as:
- Executor of a deceased person's estate
- A person with authority to act as personal rep for an adult or emancipated minor

EXCEPTIONS:

- When the individual is an unemancipated minor ,and, under applicable law:
    - The minor consents to the health care service and no other consent is required by law
    - The minor has not requested a personal rep be involved
    - The minor , a court, or other person authorized by law may lawfully consent to the healthcare service (without parental consent)
    - The parent "assents to an agreement of confidentiality" between the provider and the minor with respect to the health care service

- When the individual "has been or may be subject to abuse, neglect, endangerment" by the personal rep., and the entity has reasonable belief that treating such person as the individual
    - Could endanger the individual
    - Would not be in the best interest of the individual (in the entity's professional judgment).

Disclosures by whistleblowers and workforce member crime victims

Disclosure by whistleblowers is OK if:

- Workforce member or business associate believes the covered entity is engaged in unlawful conduct that violates professional / clinical standards, or that endangers patients, workers, or the public

And the disclosure is provided to:

- Health oversight agency or public health authority that oversees the covered entity
- An attorney retained by the whistleblower

Note: Under the Federal whistleblower statute, the whistleblower is entitled to 15% of the judgment $$.

164.504 Uses and disclosures: Organizational requirements

Definitions:

Common control	An entity that has the power to direct actions or policies of another entity
Common ownership	An entity that has 5% or greater ownership or equity in another entity.
Health care component	Components of a covered entity that perform covered functions. Also: Where a component performs covered functions that would make it a business associate of the other component if they were separate legal entities; and The activities involve use/disclosure of protected health information.
Hybrid entity	A single legal entity that is a covered entity, but the covered functions are not its primary functions.
Plan administration functions	Functions performed by the plan sponsor on behalf of the health plan.
Summary health information	Information that may be PHI, and summarizes claim history, payment history, or claim type for individuals, that has been de-identified except for a five-digit zip code.

Hybrid entities: safeguards and requirements

- The (covered) hybrid entity must ensure that the health care component does not disclose protected health information to the non-healthcare component of the entity.
- When an employee works for more than one component of a hybrid entity, the employee may not disclose to the non-healthcare part of the business.

- Hybrid entities must comply with Section 160 and must implement all policies and procedures required in section 164.530(i). The covered entity must designate all healthcare components of the business and maintain documentation of this designation in written or electronic form.

Affiliated covered entities: Requirements
Legally separate covered entities may designate themselves as affiliate entities if they are all under common ownership or control. Documentation (written or electronic) of this designation must be maintained. The affiliate entity must comply with all requirements of this subpart.

Business Associate Contracts: Requirements
A contract between the covered entity and business associate must:
- Establish the permitted and required uses and disclosures
- Associate must not use or further disclose information other than what's permitted by the contract or by law
- Use appropriate safeguards to protect the information exchanged
- Report any use/disclosure to the covered entity that is not provided for in the contract
- The BA agreement also applies to agents and subcontractors of the business associate
- Agreement must include provisions on amendment / correction of medical information, and accounting of disclosures
- BA agrees to make all of its internal practices, books, and records relating to protected information available to the Secretary for determining compliance
- If feasible, at termination of contract, return or destroy all protected health info maintained by the BA. If return/destruction is not feasible, then contract protection continues indefinitely for this information.
- Covered entity can terminate at any time if BA has violated the contract.

Business Associate Contracts: Other Arrangements
If a covered entity and its business associate are both governmental entities, they may comply with a MOU that is compliant with this section (in lieu of the "standard" BA contract). The termination authorization may be omitted if this would be inconsistent with the statutory obligations of either partner.

Other requirements for contracts and other arrangements:
BA may use information received from the covered entity as necessary
- For management / administration of the BA
- To carry out legal responsibilities of the BA
- BA may disclose, with proper consent present, provided that
    - Disclosure is required by law, or
    - Reasonable assurance exists that the information will only be used for the intended purpose
    - Person will notify the BA if a breach of confidentiality occurs

Requirements for group health plans
Plan documents must be compliant with this subpart, in order to permit disclosure to the plan sponsor by a health insurance issuer / HMO /group health plan.

Summary health information may be disclosed for purposes of obtaining premium bids, or modifying the group health plan.

Plan documents of group health plans may require revisions. The plan sponsor must:
- Only use information only as permitted by law
- Ensure that agents / subcontractors agree to the same restrictions/conditions
- Not use / disclose in any employment-related actions
- Report any violations it becomes aware of
- Comply with requirements re: availability / amendment and correction / accounting of disclosures /books and records availability / return or destruction of records at termination of sponsorship.

- Provide for adequate separation between the group health plan and the sponsor, detail responsibilities of employees to protect PHI
- Provide mechanism for resolving noncompliance issues.

164.506 <u>Consent</u> for uses and disclosures to carry out treatment, payment, and health care operations (please see note, section 164.508)

<u>Requirement:</u>
Health care provider ***<u>must obtain individual's consent for treatment, payment, and health care operations</u>***.

- A covered health provider may condition treatment on obtaining consent. The covered entity is permitted to not treat an individual if a consent is not obtained.
- A health plan may condition enrollment on obtaining a consent.
- The consent form may not be combined with the entity's privacy statement (ref.164.520).
- The consent form may be combined with "consent for treatment" or "assignment of benefits", provided that the consent form is "visually separate" and separately signed and dated by the individual.
- The consent form may be combined with a research authorization (ref. 164.508).
- Consent may be revoked (in writing) at any time
- Covered entity must retain the signed consent documents.

<u>Exceptions to consent requirement:</u>

- Provider has an indirect treatment relationship with the individual
- Treatment is being provided to an inmate
- Emergency treatment situation (obtain consent as soon as feasible)
- When provider is required to treat individual by law, and provider unable to obtain consent
- A communication barrier exists between patient and provider, but provider judges that consent is "inferred" under the circumstances

<u>Consent content requirements, Required Elements:</u>
Consent form must be in plain language, and

- Inform individual that info may be used / disclosed to carry out treatment, payment, healthcare operations
- Refer individual to privacy policy for more information, and that the individual has a right to review the privacy statement before signing the consent
- If the terms of the consent or privacy policy of the covered entity should change, describe how the individual can obtain a revised notice.
- Inform individual of the right to restrict how their health info is used
- Covered entity does not have to agree to the restriction, but if it does, the restriction is binding on the covered entity
- Individual's right to revoke consent in writing
- Be signed and dated by the individual.

<u>Defective Consents.</u>
The consent is considered invalid if it lacks a required element as described above, or if the consent is revoked by the individual.

<u>Resolving conflicting consents and authorizations</u>
If a covered entity receives more than one consent from an individual, the entity may only disclose per the more restrictive consent. Conflicts may be resolved by:

- Obtaining a new consent
- Communicating with the individual to determine his/her preference, document the preference, then only disclose per the preferred consent agreement.

Joint consent; requirements

- Consent must include the name(s) of all covered entities that the joint consent applies to
- Modify other sections of the consent form as necessary to include each of the covered entities.
- If consent is revoked, the covered entity receiving the revocation must inform the other entities.

164.508 Uses and disclosures for which an authorization is required

Note: *A consent is written in general terms, allowing use/disclosure by the covered entity for treatment, payment, health care operations ONLY. In contrast, an authorization must be written in very specific terms and allows use / disclosure for purposes other than those covered by the consent.*

Psychotherapy notes
Individual authorization is required.

Exceptions to authorization requirements: To carry out the following uses (permitted) for treatment, payment, healthcare operations:

- Use by the originator of the notes for treatment
- Use by the covered entity for training/educational purposes
- To defend a legal action brought by the individual
- Disclosure required by law
- Use for health oversight of the psychotherapy notes' originator
- Use by coroner / medical examiner
- Threat to health and safety exists for the public or the individual

Valid authorizations
Must contain each of the required elements listed in 164.506, and may contain additional elements.
Defective authorizations
Authorization is defective if it is expired, not filled out completely, lacks a required element, or contains information known by the covered entity to be false.
Compound authorizations
An authorization may not be combined with another authorization, except:

- Authorization for research that includes treatment of the individual
- Can combine an authorization for disclosure of psychotherapy notes only with another authorization for disclosure of psychotherapy notes

Prohibition on conditioning of authorizations
Covered entity may not condition the provision of treatment, payment, enrollment, or eligibility on getting an authorization from the individual, EXCEPT:

For research-related treatment
Health plan can request authorization prior to enrollment for underwriting / risk rating
The authorization is not for disclosure of psychotherapy notes
Health plan can condition claim payment if:
Disclosure is necessary to pay the claim
Authorization is not for disclosure of psychotherapy notes

Revocation of authorizations
An authorization may be revoked by the individual in writing at any time.

Documentation requirements
Covered entity must retain documentation

Authorizations; core elements and requirements

- Specific description of information to be used
- Identify persons authorized to disclose / use the information
- Expiration date of authorization

- Right to revoke authorization
- Information disclosed may be subject to re-disclosure and no longer protected by this rule
- Signature of the individual, and date
- If personal rep involved, describe the authority of the personal rep

Plain language requirement
Authorization must be in plain language. Provide a copy to the individual.

Information created for research that includes treatment of the individual.
Individual's authorization is required. A majority of the IRB or privacy board can approve a waiver, using an expedited review process if necessary.

Use / disclosure to avert serious threat to health or safety

Permitted	**Not Permitted**
Serious and imminent threat to health / safety of public or individual exists	
Disclosure is to a person able to prevent / lessen the threat	
Disclosure necessary for law enforcement to identify/apprehend an individual	
Individual has admitted participation in a violent crime causing serious harm to victim. Disclosure is limited to the individual's statement and related protected information	If the treatment is to lessen the propensity to commit the conduct that is the basis for disclosure, or the individual has requested treatment be initiated.
Individual has escaped from correctional facility	

Use / disclosure for specialized government functions
OK to disclose PHI of Armed Forces personnel if deemed necessary by appropriate military authority, IF the authority has published notice in the Federal Register of who the appropriate authority is, and the purpose for use/disclosure of the PHI. {Also applies to foreign military personnel.}

May disclose to Dept. of Veterans Affairs after separation from military service, for the purposes of obtaining entitlement to benefits.

National security and intelligence activities
Covered entity OK to disclose, under National Security Act and per Executive Order 12333.

Protective services for the President, foreign heads of state, and others
Covered entity OK to disclose

Medical suitability determinations, Department of State
Covered entity component of Department of State OK to use / disclose for:
- Required security clearance
- As necessary to determine availability for mandatory service abroad
- For a family to accompany Foreign Service member abroad

Correctional Institutions and other custodial situations
Covered entity OK to disclose an inmate's health info to a correctional institution or law enforcement official having custody for:
- Provision of healthcare
- Health and safety of individual / other inmates / officers / employees / individuals who transport inmates

This provision no longer applies to an individual once (s)he is released on parole, probation

Covered entities that are government programs providing government benefits

Entity	**May disclose to:**
Government program (health plan) providing public benefits	Another agency that administers the government program providing public benefits
Covered entity (government agency administering program)	Another agency provided that they serve the same or similar populations
Covered entity	Workers' comp or similar programs established by law that provide benefits for work-related injury

164.510 Uses and disclosures requiring an opportunity for the individual to agree or object
A covered entity may use or disclose for the following as long as the individual is informed in advance and has the right to agree to, or prohibit, or restrict the disclosure:
To maintain a directory of individuals in its facility,

- Name of individual
- Location of individual in the facility
- The individual's condition, described in general terms
- The individual's religious affiliation (to disclose only to members of the clergy)

To disclose name, location, general condition to other persons who ask for the individual by name.

If the individual is incapacitated at the time of admission, provider may disclose:
If individual's prior preference is known
In the provider's professional judgment, the disclosure is in the individual's best interest
Individual must be provided the opportunity to object as soon as practicable to do so.

Uses and disclosures for involvement in the individual's care, and for notification purposes
A covered entity may disclose directly relevant PHI to:

- Family member
- Other relative
- Close personal friend
- Other person identified by the individual

for the care of the individual or payment related to the individual's health care.

If the individual is present, and not incapacitated, the covered entity may use/disclose with the individual's agreement. Entity must give the individual an opportunity to object, or reasonably infer that the individual does not object to the disclosure.
If the individual is incapacitated, covered entity may use its professional judgment to make a reasonable inference as to the individual's best interest.
Covered entity may disclose PHI to notify, or assist in the identification of a family member, personal rep, or other individual responsible for the care of the individual of the individual's location, general condition, or death.

Use and disclosure for disaster relief purposes
Covered entity may disclose PHI to a disaster relief agency in emergency circumstances. The "opportunity to object" requirement cannot interfere with the ability to respond in an emergency.

164.512 Uses and disclosures for which a consent, an authorization, or the opportunity to agree or object is not required
Pertains to uses and disclosures required by law.

Permitted uses and disclosures for Public health activities:
Preventing or controlling disease, injury, or disability
Vital events (birth, death)
Public health surveillance, investigations, interventions

To a public health or other government agency authorized by law to receive reports of child abuse or neglect
To an official of a foreign government agency acting in collaboration with a public health authority
To a person subject to jurisdiction of the FDA
To report adverse events, product defects
To enable product recalls, or conduct post marketing surveillance to comply with the FDA
To a person who may have been exposed to a communicable disease or be at risk
To an employer, to conduct an evaluation of medical surveillance of the workplace
To evaluate whether an employee has a work-related illness or injury

The disclosure consists of findings regarding a work-related illness or injury
The employer needs the findings to comply with reporting requirements and carry out its responsibilities for workplace medical surveillance
The covered health care provider gives notice of disclosure to the employee at the time of care
If the care is provided at the work site, post the disclosure notice in a prominent location where the care is provided.

<u>Disclosures about victims of abuse, neglect, or domestic violence</u>
If covered entity reasonably believes that the individual is a victim of abuse, neglect, or domestic violence, it may disclose to a government authority, including a social service or protective agency:

- To the extent required by law
- If the individual agrees to the disclosure; or
  To the extent authorized by statute or regulation, if the covered entity believes the disclosure is necessary to prevent serious harm to the individual or other potential victims
- If the individual is incapacitated, and an immediate law enforcement activity would be adversely affected by waiting for the individual to be able to agree to the disclosure, entity may disclose.

The covered entity must inform the individual that a report of abuse has been made, except:

- If the covered entity believes that informing the individual would put him/her at risk of serious harm
- If the covered entity would be informing the individual's personal rep, and it believes that the personal rep is responsible for the abuse/neglect/injury of the individual

<u>Permitted uses and disclosures for health oversight activities</u>
Covered entity may disclose PHI to a health oversight agency for:

- Audits
- Civil, administrative, or criminal proceedings or actions
- Activities necessary for oversight of:
  The healthcare system
  Government benefit programs
  Entities subject to government regulatory programs
  Entities subject to civil rights laws

where health information is necessary for determining compliance.

<u>Permitted disclosures for judicial and administrative proceedings</u>
Covered entity may disclose:
In response to a court order, subpoena, discovery request
If the covered entity has reasonable assurance that:

The requesting party has made a good faith attempt to provide written notice to the individual prior to making the request
The individual had an opportunity to object to the disclosure
No objections were filed
Objections filed have been resolved
Parties to the dispute have agreed to a qualified protective order, meaning:

PHI can only be used for the litigation for which the info was requested
PHI must be destroyed or returned to the covered entity at the end of the litigation

Permitted disclosures pursuant to process and as required by law

- For the reporting of certain types of wounds or other physical injuries
- In compliance with:
  - A court order or subpoena or summons
  - A grand jury subpoena
  - Administrative request, subpoena, or summons
  - Civil or authorized investigative demand

AND:

- The information requested is relevant and material
- The request is limited in scope
- De-identified information could not be used.

Permitted disclosures for identification and location purposes:

In addition to other disclosures required by law, a covered entity may disclose to law enforcement about:

Whom	**What can be disclosed**
Suspect, fugitive, material witness, missing person	Name and address Place and date of birth Social security number ABO blood type and rh factor Type of injury Date and time of treatment Date and time of death Description of distinguishing physical characteristics
	What cannot be disclosed (unless pursuant to process or otherwise required by law)
	Information related to the individual's DNA or DNA analysis Dental records Typing, samples, or analysis of body fluids or tissue

Permitted disclosure: crime victims

Covered entity may disclose to law enforcement if:

- The individual agrees
- Covered entity cannot obtain individual's agreement because of incapacity or emergency circumstance
- Law enforcement believes a crime has been committed against the individual
- Law enforcement activity would be adversely affected by waiting until the individual is able to agree
- Disclosure would be in the best interest of the individual (per professional judgment)

Permitted disclosure: decedents

May disclose to law enforcement if covered entity suspects that the death may have resulted from criminal conduct

Permitted disclosure: crime on premises

May disclose if entity believes evidence exists of criminal conduct on the premises of the covered entity.

Permitted disclosure: reporting crime in emergencies

May disclose:
Commission and nature of a crime
Identity, description, location of the perpetrator
(If the crime is the result of abuse, neglect, or domestic violence, does not apply to this section)

Uses and disclosures about decedents

May disclose to:	**In order to:**	**Subject to:**
Coroners and medical examiners	Identify deceased person Determine cause of death	

	Other duties authorized by law	
Funeral directors	Carry out duties with respect to the decedent	The death of the individual. May disclose in reasonable anticipation of the individual's death.
Cadaveric organ, eye, tissue donation organizations	Facilitate organ donation and transplantation	
Researchers		• Board approval of a waiver of authorization by an IRB or privacy board • Information is necessary for the research purpose and could not be done without the waiver • No PHI is to be removed from the covered entity • Adequate plan to protect identifiers from improper use

164.514 Other requirements relating to uses and disclosures of protected health information

Prior to any disclosure permitted by this subpart, the covered entity must verify the identity of the person making the request for protected health information by obtaining reasonable documentation/credentials, or reliance on the exercise of professional judgment.

<u>De-identification of protected health information</u>
Covered entity may determine that health info is not identifiable **if:**

- A person with appropriate knowledge of statistics / scientific principles determines that the risk is very small that the info could be used to re-identify an individual, and documents the methods used in the risk analysis.
- The following identifiers of the individual, and relatives/household members, or employers are removed:
  - Names
  - Addresses: email, URL, IP, street address, city, county/precinct. May use first 3 digits of zip code if all zip codes with those first 3 digits combined totals more than 20,000 people. If result is less than 20,000, change first 3 zip code digits to 000.
  - All elements of dates directly related to an individual
  - Numbers: phone, fax, Social Security, medical record, beneficiary number, account number, license number, vehicle id/serial#/license plate, device id/serial#
  - Biometric identifiers (voice or finger prints), full face photographs
  - Any other unique identifying number, characteristic, or code

<u>Re-identification of protected health information</u>
Covered entity may assign a code it may use to re-identify, if:

- Covered entity does not disclose the code to others
- Code was not derived from the individual's information and can't be translated in order to identify the individual

<u>Minimum necessary requirements</u>
A covered entity must:

- Identify all employees who need access to PHI, and identify all categories for access
- Make reasonable effort to restrict access as appropriate
- Minimum necessary applies to routine disclosures.

For all other disclosures, a covered entity must:

- Apply its "minimum necessary" criteria to all requests for disclosure on an individual basis

- Assume that the request meets "minimum necessary" if requested by:
  - Another covered entity
  - Workforce member or business associate of the covered entity
  - Researcher who provides documentation that complies with 164.512(i)
- Not request an individual's entire medical record unless justified as "minimum necessary" to accomplish the purpose of the request.

Uses and disclosures related to marketing; requirements

Covered entity must obtain a specific authorization from the individual.

Exceptions:

- Covered entity may discuss products / services during a face-to-face encounter, provide products / services of nominal value (calendars, pens, samples, or similar item that promotes the covered entity)
- Covered entity may target marketing materials to patients if
  - The covered entity determines that the product/service may be beneficial to the patient
  - The marketing materials must state why the individual was targeted and the benefits of the product/service
  - Allow individuals to opt-out of receiving future marketing communications

Use / disclosure related to fundraising; requirements

Covered entity may disclose to a business associate or institutionally related foundation without authorization:

Demographic information relating to an individual
Dates of healthcare provided to an individual

If any other protected health information is to be used for the fundraising effort, consent of the individual is required. Individuals must be provided information on how they can opt-out of receiving further fundraising materials.

Use / disclosure for underwriting purposes

Information received for underwriting, premium rating, or other contract-related activities may not be used for any other purpose.

164.520 Notice of privacy practices for protected health information

A covered entity must retain a copy of its privacy notice to document compliance.

An individual has a right to receive notice of how their information will be used, what the individual's rights are, and what the covered entity's legal duties are in protecting the information.

Exceptions:

- Group health plans are required to maintain a notice of privacy practices and provide it upon request to any person.
- Inmates do not have a right to notice

Content of notice; requirements

- Notice must be written in plain language and contain the following elements:
  (Statement in Header) "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."
- A description, and at least one example, of how the information may be used for payment, treatment, healthcare operations
- Description of other purposes for disclosure where consent or authorization is not required
- If a "more stringent" State law applies to use/disclosure, the entity's privacy statement must reflect the more stringent law's requirements
- A statement that other uses/disclosures will only be made with individual's authorization, and that an authorization may be revoked at any time.

Additional elements of privacy statement (if applicable to entity):

- The entity may contact the individual to provide:
  - Appointment reminders
  - Information about treatment alternatives, other services that may be of interest
  - Information about fundraising activities
  - Health plan may disclose to plan sponsor

Individual rights; Required statements:
- Right to restrict, plus a statement that the covered entity does not have to agree to the restriction
- Right to receive confidential communications
- Right to inspect, copy (164.524) amend one's health information (164.526)
- Right to an accounting of disclosures (164.528)
- Right to a paper copy of privacy notice, if notice was received electronically

Covered entity's duties; Required statements:
- Covered entity required by law to maintain privacy of protected information, provide notice of legal duties and privacy practices to individuals.
- Covered entity is required to abide by the terms of the notice.
- Covered entity reserves the right to change the terms of the notice, and how revised notice will be provided to individuals.
- That individuals may file a privacy complaint with the covered entity and/or the Secretary, how to file a complaint
- That individuals filing complaints will not be retaliated against
- Provide name, title, and contact information for privacy officer
- Effective date of notice

Provision of notice; requirements
Covered entity must provide notice to the individual:
- No later than the (privacy rule) compliance date for the health plan
- At time of enrollment
- Within 60 days of revising the notice
- At least once every 3 years
- At the time of service (provider that has a direct treatment relationship)
- Have copies of the notice available at service location (office, clinic, facility), and post in conspicuous location
- If covered entity maintains web site, post notice on the web and make notice available electronically.
- OK for covered entity to transmit notice via email if the individual agrees to it.
- Individual has right to a paper copy of the notice

Joint notice by separate covered entities; requirements
- Entities agree to abide by terms of notice
- Required statements may be altered to show that notice applies to more than one entity
- Description of who the covered entities are
- Describe the delivery sites the notice applies to
- If organized health care arrangement, describe that information may be shared to carry out treatment/payment/operations

164.521 Rights to request privacy protection for protected health information
Covered entity must permit an individual to restrict disclosure to carry out treatment / payment / healthcare operations
The Covered entity does not have to agree to a restriction
A covered entity that does agree to a restriction may use the information if it becomes necessary for emergency treatment.
A covered entity may terminate its agreement to a restriction, if:
- The individual agrees in writing

- The individual orally agrees, and the restriction termination is documented in writing
- Covered entity informs the individual of the termination. Information the entity already possesses is still protected (restricted).
- Entity must document the restriction agreement in writing.

Confidential communications; requirements
Covered entities must accommodate reasonable requests for individuals to receive communications by alternative means or at alternative locations. Entity may require that this request be in writing.

164.524 Access of individuals to protected health information
Individual has the right to access and obtain a copy of their protected health information.
Exceptions:
- Psychotherapy notes
- Information compiled for use in a civil, criminal, or administrative proceeding
- A correctional institution (or provider acting on institution's behalf) may refuse inmate's request
- Information created in the course of research still in progress
- If access would be denied under the Privacy Act, section 552a
- If information was obtained under a confidentiality agreement from someone other than a provider, and giving access to the individual would reveal the source of the information
- If access is reasonably likely (per professional judgment) to endanger the life or safety of the individual or another person
- The request was made by an individual's personal representative, and giving the rep access to the information (per professional judgment) is likely to cause harm to the individual or other person.

Denied access: Appeal process
The individual who is denied access is entitled to have the denial reviewed by a licensed health care professional designated by the covered entity to act as a reviewing official. The covered entity must abide by the reviewer's decision. The official must not have participated in the original decision to deny access

Timely action
Covered entity must respond to access request within 30 days of receipt
May have up to 60 days if information is not maintained onsite
May only extend the time once, and provide the individual with a written statement of the reasons for the delay and inform the individual when the request will be completed.

Providing access to information
Covered entity must:
- Provide the information in the format requested by the individual, if possible; otherwise, a hard copy is OK.
- Provide a convenient time /place for individual to obtain the information, or mail the information on request.
- For copying or providing a summary of requested information, the entity may charge a reasonable fee that includes only the cost of:
    - Copying, supplies for copying, labor, postage, preparation of summary (if requested).

If a covered entity does not maintain the information that is the subject of the request, but does know where it is maintained, the covered entity must direct the individual to the right place.

Documentation
The covered entity must create / maintain documentation of:
- Designated record sets that are subject to access by individuals
- Persons or offices responsible for handling access requests

164.525 Amendment of protected health information
Requirements:

The covered entity must permit individuals to request amendment of their health information
May require request to be in writing, and contain a reason why the information should be amended
Entity must respond within 60 days of receiving amendment request, and may extend time limit only once.
If the amendment is accepted by the covered entity, it must:

- Identify the section(s) of the document affected by the amendment
- Obtain permission from the individual to share amended information with relevant persons (including business associates)

Denial:
If the amendment is denied, covered entity must provide:

The basis for the denial, in plain language
Statement of the individual's right to submit a written statement disagreeing with the denial, and that:

- Covered entity may limit the length of this statement.
- Covered entity may prepare a rebuttal to the individual's statement of disagreement.
- Individual can ask that the amendment request (and its denial) be included with any future disclosures of the protected health information in question
- Individual may file a complaint with the Secretary. Provide the individual with a name, title, and contact information to assist in doing so.

A covered entity must retain documentation of the titles of persons or offices that handle amendment requests.

When covered entity "A" is informed by covered entity "B" that there has been an amendment to an individual's record, entity A must also amend its record.

164.528 Accounting of disclosures of protected health information
An individual has a right to an accounting of disclosures made by a covered entity, going back as far as six years from the date of the request.
Exceptions:

- Disclosures to carry out treatment, payment, and healthcare operations
- Disclosures to individuals of protected information about them (164.502)
- Disclosure for the facility's directory or to persons involved in the individual's care, or other notification purposes outlined in 164.502
- Disclosure for national security or intelligence purposes (164.512 k 2)
- Disclosure to correctional institutions or law enforcement
- Disclosures that occurred prior to the compliance date

Content of the accounting
For each disclosure, include:

- Date of disclosure
- Name and address of person/entity who received the information
- Brief description of what was disclosed
- Purpose of disclosure
- OR:
- Copy of individual's written authorization for disclosure.
- If multiple disclosures to the same entity for the same purpose, indicate frequency or number of disclosures made during the accounting period and date of last disclosure

Covered entity may extend time period for providing the accounting only once, by no more than 30 days.
Must provide first accounting to an individual once in any 12-month period without charge. After that, entity may charge a reasonable fee. Must give individual the opportunity to withdraw or modify the request to avoid the fee.
Entity must document and retain the written accounting provided to an individual

Retain documentation that indicates the titles of the persons or offices responsible for the accounting function

164.530 Administrative requirements

A covered entity must designate:

A privacy official who is responsible for development and implementation of privacy policy/procedures

A person or office responsible for handling privacy complaints

Compliance training:

Covered entity must train all members of its workforce on privacy compliance

- By no later than the compliance date
- To each new hire within a reasonable period of time
- To each member of the workforce after a material change in policies and procedures
- The provision of training must be documented

Safeguards:

- Covered entity must have appropriate administrative, technical, and physical safeguards to protect the privacy of health information.
- Covered entity must reasonably safeguard protected information from unintended use/disclosure.
- Covered entity must provide a complaint process, and document all complaints received and their disposition

Sanctions

Covered entity must have and apply appropriate sanctions against employees who fail to comply with privacy policies and procedures. Entity must document any applications of these sanctions.
Covered entity must mitigate harmful effects of any disclosure that is in violation of policy.

Refrain from intimidating or retaliatory acts

Covered entity may not retaliate against individuals for:

Filing a complaint

Testifying, assisting, participating in an investigation or compliance review

Opposing any practice that the individual believes is unlawful

Covered entity cannot require individuals to waive their right to file a complaint with the Secretary as a condition for provision of treatment, eligibility, or enrollment in a health plan

Changes in law

When there is a change in privacy law, the covered entity must document and promptly implement the revised policy or procedure. If applicable, privacy notice must be revised per section 164.520.
Documentation must be retained for six years.

Exception for group health plans

This section does not apply to group health plans that do not create or receive protected health information, except for summary information and enrollment information

164.532 Transition provisions

Prior to the required compliance date:
A covered entity may continue to use / disclose per existing agreements
Must continue to comply with any existing consent limitations obtained from an individual

164.534 Compliance dates for initial implementation of the privacy standards

Large health plans and clearinghouses: February 26, 2003
Small health plans: February 26, 2004